

A method of remote loading of confidential information between a secure pin entry device and a Authorizing Institute using public and private key encryption techniques. In addition, a digital certificate uniquely identifying the terminal is provided by the terminal when a communication with the Authorizing Institute is originated. The Authorizing Institute confirms the authenticity of the digital certificate. This confirmation can occur using the public key of the Certificate Authority and/or confirmation can be made by contacting the Certificate Authority. In this way, confidence to use the public and private keys of the device and the Authorizing Institute for encryption is achieved, and financial keys and/or software can be encrypted downloaded to the device.